問3　リモートアクセス環境の情報セキュリティ対策に関する次の記述を読んで，設問1～4に答えよ。

H社は，従業員数600名の産業用機械製造・販売会社であり，本社と8か所の支店がある。H社では，全従業員に1台ずつデスクトップPCを貸与している。他拠点への出張が多い従業員と，外出が多い営業部員には，社外持出し用PCも貸与している。社外持出し用PCは，出張先で業務システムから業務データを取り出せるように，拠点の社内LANに接続して業務システムを使うことが許可されている。

また，営業部員にはリモートアクセス環境が提供されている。H社には20の業務システムがあり，全てデータセンタ（以下，DCという）に設置されているが，現在リモートアクセス環境で利用できる業務システムは，営業支援システムだけである。

現在H社では，PC管理の効率化，及び従業員の利便性向上を目的として，デスクトップ仮想化によるシンクライアント環境（以下，VDIという）の導入の準備をしており，社内で利用しているデスクトップPCをVDIに置き換えることが，既に決定している。H社のVDIの概要を図1に示す。

(a) 仮想化ソフトウェアが動作するサーバ（以下，VDIサーバという）がDCに設置されており，その上で最大50台まで稼働する仮想化されたPC（以下，V-PCという）に，利用者がクライアント端末から接続する。
(b) 社内で利用しているデスクトップPCは全て回収し，デスクトップPC型のシンクライアント端末（以下，DTという）を全従業員に貸与する。また，①本社及び支店に，共用端末として数台のDTを設置し，他拠点から出張中の従業員が利用できるようにするとともに，出張時のPC利用に関するルールを設ける。
(c) DTからV-PCにキーボード及びマウスの入力が送信され，V-PCからDTに画面情報が送信される。
(d) 管理者は，ウイルス対策ソフトがインストールされ，ウイルス定義ファイルの自動更新が有効にされたマスタイメージを作成する。
(e) 利用者は，管理者が最新のマスタイメージから複製するV-PCを利用する。
(f) V-PCを利用するには，DTからV-PC接続ソフトを使って，VDI接続サーバに接続する。VDI接続サーバは利用者を認証した後で，DTとV-PCを接続する。
(g) VDI接続サーバでの利用者認証後，シングルサインオンによって，利用者は自動的にV-PCにログオンするとともに，追加の利用者認証なしで全ての業務システムを利用できる。
(h) 利用者がV-PCをログオフすると，そのV-PCは解放され，複製時の状態に初期化される。次回のログオン時には初期化されたV-PCに接続される。
(i) 利用者がV-PCをログオフせずに，V-PC接続ソフトを終了するか，又はDTの電源を切ると，V-PCの状態は維持され，次回の接続時にはそのV-PCに接続される。
（以下，省略）

図1　VDIの概要

〔リモートアクセス環境改善の要望〕

営業部では以前から，リモートアクセス環境で利用できる業務システムが限られていることに対する不満が挙がっていた。VDI 導入の決定を受けて，営業部長は情報システム部の K 部長に対して，“VDI の導入に合わせてリモートアクセス環境も強化し，勤怠管理・経費精算を行う業務管理システムと，電子メール（以下，メールという）も社外から利用できるようにしてほしい”という要望を出した。

K 部長は，営業部の要望を受け入れて，情報システム部の N 主任に，リモートアクセス環境の改善を検討するように指示した。改善案には，リモートアクセス特有のセキュリティ上のリスクへの対策も含めるように指示した。

〔リモートアクセス環境改善の検討〕

N 主任は，改善案として，VPN を利用してリモートアクセスを行う案（以下，案 1 という）と，VDI を利用してリモートアクセスを行う案（以下，案 2 という）を検討した。それぞれの案の概要を図 2 及び図 3 に示す。

- 社外持出し用 PC に VPN 接続ソフトをインストールし，DC に設置した VPN 装置に接続する。
- VPN 装置での ID とパスワードによる利用者認証後，社外持出し用 PC から直接業務システムにアクセスする。
- 社外持出し用 PC から VPN を利用して，営業支援システムのほか，業務管理システムとメールサーバにアクセスできる。
- VPN 接続後，業務システムごとの利用者認証に成功すると，業務システムを利用できる。
- 社外持出し用 PC では，修正パッチの自動適用と，ウイルス対策ソフトのウイルス定義ファイルの自動更新を有効にする。

図 2　案 1 の概要

- 社外持出し用 PC の代わりに，ノート型のシンクライアント端末（以下，NT という）を使用し，DC に設置したゲートウェイサーバ（以下，GW サーバという）に接続する。
- GW サーバでの ID とパスワードによる利用者認証後，シングルサインオンによって VDI 接続サーバの利用者認証が自動的に行われ，NT から V-PC に接続する。
- NT から，V-PC を使って間接的に業務システムを利用する。
- NT と GW サーバの間の通信は暗号化する。

図 3　案 2 の概要

N 主任はさらに，案 1 と案 2 について，リモートアクセス特有のリスクに対するリスク評価を行い，対策案を検討した。リスク評価の結果を表 1 に，リスクへの対策案を表 2 に示す。

表1　案1と案2それぞれのリスク評価の結果

リスク		リスク評価	
		案1	案2
(ア)	リモートアクセス通信経路での盗聴による情報漏えい	社外持出し用 PC と VPN 装置との間の通信が暗号化されているので，リスクは小さい。	NT と GW サーバとの間の通信が暗号化されているので，リスクは小さい。
(イ)	なりすましによるリモートアクセス環境への不正接続	VPN 装置がインターネットに公開されるので，リスクが大きい。	GW サーバがインターネットに公開されるので，リスクが大きい。
(ウ)	社外持出し用 PC 又は NT の盗難・紛失による情報漏えい	[a] が社外持出し用 PC に保存される可能性があるので，リスクが大きい。	V-PC 利用時は [a] が NT に残らないが，V-PC 以外の利用によって保存される可能性があるので，リスクが大きい。
(エ)	ウイルスの感染	社外持出し用 PC が長期間使用されていない場合，リスクが大きい。	図 1 の(e)の運用が確実でない場合，リスクが大きい。

表2　リスクへの対策案

リスク	リスクへの対策案	
	案1	案2
(ア)	－	－
(イ)	VPN 装置での利用者認証を強化する。	GW サーバでの利用者認証を強化する。
(ウ)	社外持出し用 PC で [b] の対策を行う。	NT で案 1 と同様の対策を行う，又は，[a] の保存を制限できる機能をもつ NT を利用する。
(エ)	利用者が，社外持出し用 PC 起動時に未適用の修正パッチがないことを確認する。	管理者が修正パッチの公開を確認した後で，②直ちに実施すべき作業を定める。

注記　リスク（ア）は，リスクが小さいので対策しない。

〔検討結果に対する指摘〕

N 主任はこれらの検討結果とシステム構成図を K 部長に提出した。K 部長は案 1 と案 2 とを比較して，次の 2 点を理由に案 2 を採用すべきであると N 主任に伝えた。

・リモートアクセス特有のリスクへの対策に，VDI の仕組みを生かせる。

・現在進めている VDI 導入の投資を生かせる。

N 主任が作成した，案 2 のシステム構成図を図 4 に示す。

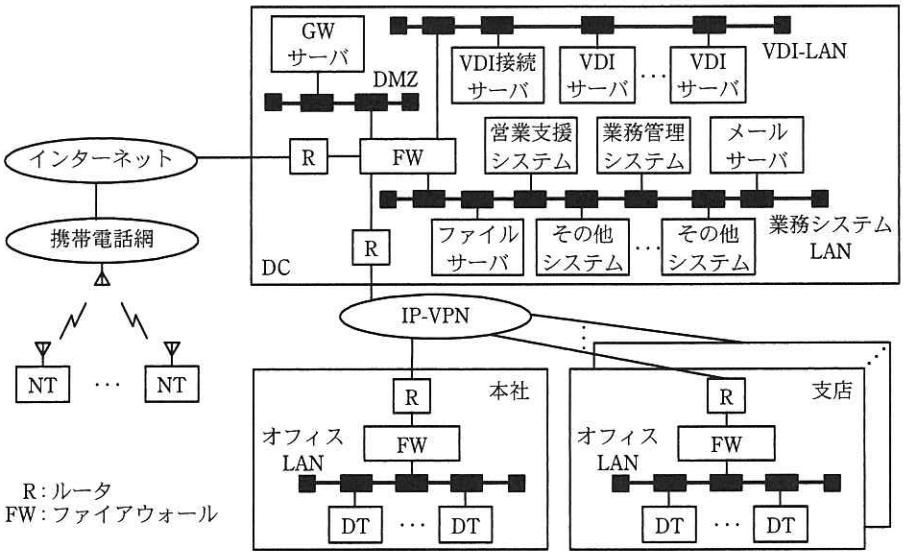

図4　案2のシステム構成図

また，K 部長は N 主任に，案 2 のリスクへの対策案は，次の点で不十分であると指摘した。

(1)　リスク(イ)が顕在化した場合，③案 1 よりも影響範囲が大きいと考えられる。より確実な対策を検討する必要がある。

(2)　リスク(ウ)への対策を確定させるために，NT の仕様を確認する必要がある。また，リスク(エ)について，NT 上のリスクと対策が考慮されていないので，対策を検討する必要がある。

(3)　VDI 導入の検討では，ネットワークのアクセス制御を変更していない。リモートアクセスの検討を行うこの機会に，VDI の仕組みをセキュリティリスクの低減に生かせるように，ネットワークのアクセス制御を変更する必要がある。

〔指摘への対応〕

N 主任は，指摘(1)への対応として，様々な利用者認証の手法を調査した結果，GW サーバの利用者認証に，ワンタイムパスワードの導入を提案することにした。次に，指摘(2)への対応に先立って NT の製品選定を行うために，市場シェアの高い V 社製の NT の仕様を確認した。V 社製の NT の仕様の抜粋を図 5 に示す。

(i) H社が現在のPCで使用しているものと同じOSが稼働し，V-PC接続ソフトがインストールされている。
(ii) ファイルシステムをもっており，データの保存ができるが，書込み制限機能を有効にすることによって，NTの電源を切ったときに，NTは初期状態に戻る。
(iii) 管理者が設定することによって，修正パッチの適用及びファイルの配信を自動で行うことができる。利用者がNTをオフィスLANに接続すると，自動的に書込み制限機能が解除され，修正パッチの適用及びファイルの配信が行われる。管理者による設定は，修正パッチの適用及びファイルの配信ごとに行う必要がある。
(iv) 管理者が設定することによって，利用者によるアプリケーションのインストールを禁止できる。

図5　V社製のNTの仕様（抜粋）

図5の仕様を調べたN主任は，V社製のNTを採用候補とした。その上で，指摘(2)への対応を検討した。

仕様(ii)の機能が，リスク(ウ)への対策として効果があると考えたN主任は，この機能を有効にするとともに，NTの利用終了時に必ずNTの電源を切ることをルール化することにした。

リスク(エ)については，NTがウイルスに感染するリスクに対する考慮が漏れていたので，このリスクに対して次の四つの対策を考えた。

(A) NTへの修正パッチの適用を，仕様(iii)の機能を使って行う。そのためにNTの管理サーバが必要になるので，VDI-LAN上に設置する。

(B) ウイルス対策ソフトをNTにインストールする。

(C) 仕様(iv)の機能を使って，V-PCへの接続に必要なアプリケーション以外はインストールさせない。

(D) NTは，V-PCの利用だけに用いる。

このうち，対策(B)については，リスク(ウ)への対策として仕様(ii)の機能を利用することを前提とした場合，高い頻度で行われるウイルス定義ファイルの更新のたびに，④管理者の作業と利用者の操作が発生してしまうので，現実的には難しいと考えた。そこで，対策(A)，対策(C)及び対策(D)をリスク(エ)への対策とすることにした。

最後にN主任は，指摘(3)への対応として，⑤図4中の各FWの設定を変更し，オフィスLANからアクセスできるネットワークをVDI-LANに限定することにした。

N主任は，以上の検討結果をまとめ，K部長に報告した。

〔改善案の承認〕

報告を受けたK部長は，N主任の案は，十分なセキュリティを確保し，かつリモートアクセス環境に対する営業部の要望を満たしていると判断し，採用を決定した。その後H社は，VDI導入と合わせてリモートアクセス環境の強化を行うことを決定した。

設問1　図1中の下線①によって得られるセキュリティ上の効果を，40字以内で具体的に述べよ。

設問2　〔リモートアクセス環境改善の検討〕について，(1)～(3)に答えよ。

(1)　表1中及び表2中の［　a　］に入れる適切な字句を10字以内で答えよ。

(2)　表2中の［　b　］に入れる適切な字句を15字以内で答えよ。

(3)　表2中の下線②について，管理者が実施すべき作業を三つ，それぞれ20字以内で述べよ。

設問3　本文中の下線③について，K部長が指摘した理由を，35字以内で述べよ。

設問4　〔指摘への対応〕について，(1)，(2)に答えよ。

(1)　本文中の下線④について，ウイルス定義ファイルの更新のたびに発生する管理者の作業と利用者の操作を，それぞれ25字以内で述べよ。

(2)　本文中の下線⑤について，N主任が考えたセキュリティリスク低減の効果を，30字以内で具体的に述べよ。また，そのような効果がある理由を30字以内で述べよ。